



(12) BẢN MÔ TẢ SÁNG CHẾ THUỘC BẢNG ĐỘC QUYỀN SÁNG CHẾ

(19) Cộng hòa xã hội chủ nghĩa Việt Nam (VN)
CỤC SỞ HỮU TRÍ TUỆ

(11)



1-0036511

(51)⁷ B60R 25/24

(13) B

(21) 1-2016-03274

(22) 03/02/2015

(86) PCT/KR2015/001118 03/02/2015

(87) WO2015/119417 13/08/2015

(30) 10-2014-0014459 07/02/2014 KR

(45) 25/07/2023 424

(43) 26/12/2016 345A

(76) 1. KIM, Gwang Woo (KR)

108-1403, Lotte Apt., 20-9, Daehak-ro 298-gil, Hayang-eup Gyeongsan-si
Gyeongsangbuk-do, 712-910, Republic of Korea

2. CHOI, Kun Hwi (KR)

5-2304, Sungwon Apt., 14, Nongong-ro 23-gil, Nongong-eup Dalseong-gun Daegu,
711-714 Republic of Korea

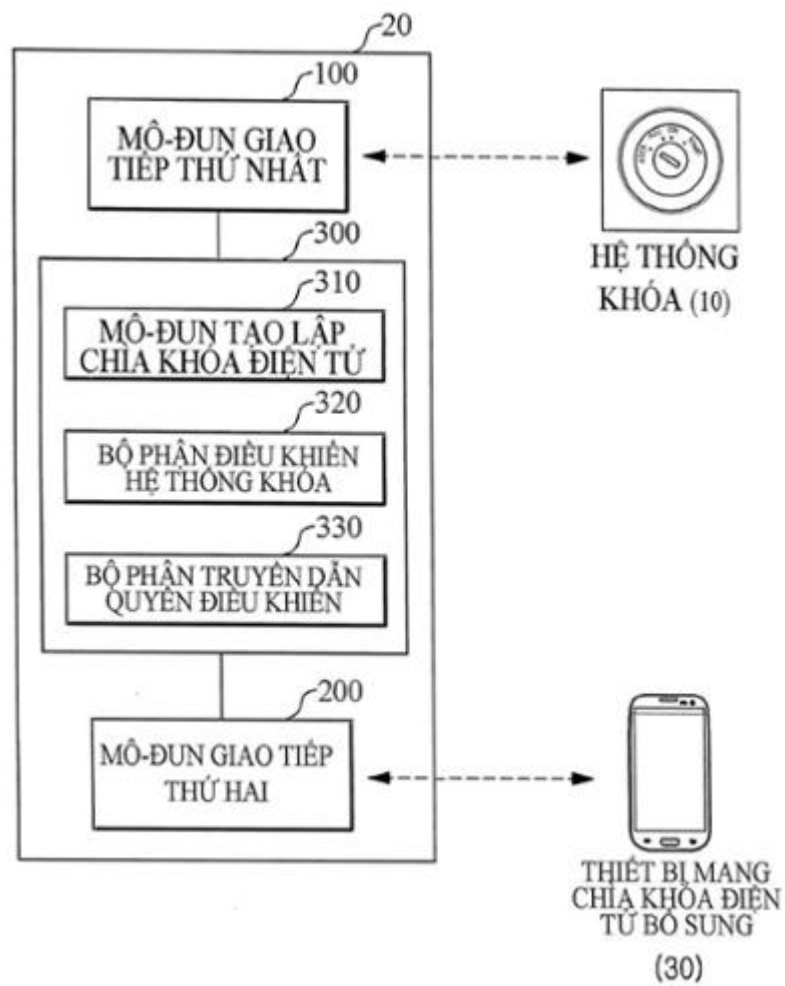
3. CHOI, Cheung Hui (KR)

(Daegok-dong, Samsung 1 Cha Raemian Apt.,)106-1602, 23, Sanghwa-ro 8-gil
Dalseo-gu Daegu, 704-723 Republic of Korea

(74) Công ty TNHH Tư vấn ALIATLEGAL (ALIAT LEGAL)

(54) THIẾT BỊ MANG CHÌA KHÓA ĐIỆN TỬ

(57) Sáng chế đề cập đến thiết bị chìa khóa điện tử có khả năng điều khiển không dây và gửi quyền truy cập để điều khiển hệ thống khóa, và hệ thống chìa khóa điện tử và phương pháp tạo lập hệ thống chìa khóa điện tử được đề cập trong sáng chế, hoạt động của hệ thống khóa được điều khiển bằng cách giao tiếp với hệ thống khóa, và một chìa khóa điện tử có thể được truyền đi, được cho thuê một cách đơn giản, ở một khoảng cách xa thông qua mạng truyền thông, bằng cách giao tiếp với một thiết bị chìa khóa điện tử khác và cấp quyền điều khiển hoạt động của hệ thống khóa cho một thiết bị mang chìa khóa điện tử khác.



Lĩnh vực kỹ thuật của sáng chế

Sáng chế đề cập tới thiết bị chìa khóa điện tử, cụ thể hơn là một thiết bị chìa khóa điện tử, hệ thống khóa và phương pháp tạo lập hệ thống chìa khóa điện tử, có thể điều khiển không dây hệ thống khóa và cung cấp quyền truy cập cho phép điều khiển hệ thống khóa đó.

Tình trạng kỹ thuật của sáng chế

Chìa khóa điện tử giao tiếp với hệ thống khóa được cài đặt trong các thiết bị cơ khí có yêu cầu quyền truy cập của người sử dụng và nhằm điều khiển hoạt động của các thiết bị như khóa hoặc mở khóa các thiết bị, khởi động và kết thúc hoạt động của thiết bị và các hoạt động tương tự. Chìa khóa và hệ thống khóa điện tử thông thường sử dụng phương thức giao tiếp điện tử được cấu hình với một chìa khóa điện tử đã được đăng ký trước, do đó luôn đòi hỏi một thiết bị di động hỗ trợ cho chìa khóa điện tử (tham khảo Đơn sáng chế Hàn Quốc đã công bố số 20-2004-0017110, Đơn sáng chế Hàn Quốc đã công bố số 10-2008-7017989, và các tài liệu liên quan).

Gần đây, để giải quyết sự bất tiện khi phải mang theo một thiết bị di động hỗ trợ, phương pháp gắn chức năng chìa khóa điện tử vào các cổng thông tin giao tiếp di động đã được phát triển (tham khảo Đơn sáng chế Hàn Quốc đã công bố số 10-2005-0095260). Tuy nhiên, thiết bị chìa khóa điện tử được phát triển gần đây, có sử dụng cổng giao tiếp di động gắn với phương pháp chế tạo chìa khóa điện tử chỉ đơn thuần bằng cách kiểm tra quyền truy cập, và chìa khóa điện tử được tạo ra chỉ có thể sử dụng được cho các thiết bị tương ứng trong một phạm vi nhất định. Nói cách khác, khi chìa khóa điện tử được cho mượn để tiếp nhận dịch vụ lái xe hoặc khi cần thiết phải tiếp nhận một chìa khóa điện tử tại địa điểm xa, sự bất tiện là cần thiết phải cho mượn

hoặc đưa cho cổng giao tiếp di động tương ứng trong đó chìa khóa điện tử đã cài đặt.

Do đó, sáng chế nhằm phát triển một loại thiết bị mang chìa khóa điện tử mới có khả năng chuyển tải nhiều quyền truy cập khác nhau để điều khiển một hệ thống khóa, và cho phép cài đặt gián tiếp bằng cách tận dụng tối đa các tài nguyên của điện thoại di động thông thường.

EP 2590146 A1 bộc lộ một hệ thống thông tin liên lạc không dây bao gồm một thiết bị cầm tay và một thiết bị xe được cấu hình để truyền thông tin bao gồm cả trạng thái của xe. EP 2048627 A2 bộc lộ hệ thống thông tin liên lạc của xe bao gồm thiết bị xác thực khóa không dây cầm tay, thiết bị không dây cầm tay cung cấp quyền sử dụng cho người dùng và thiết bị viễn thông được lắp đặt trên xe bao gồm bộ thu phát RF tầm trung và bộ thu phát mạng không dây. US 2011/257817 A1 bộc lộ một hệ thống để liên lạc với một xe bao gồm một mô-đun điều khiển được trang bị đầu thu không chìa khóa từ xa (RKE) và được cấu hình để điều khiển các chức năng của xe để đáp ứng với tín hiệu RKE. US 2012/303182 A1 bộc lộ hệ thống quản lý xe thông qua role liên lạc không dây của bộ điều khiển từ xa của xe bao gồm: thiết bị đầu cuối điều khiển phương tiện được cung cấp mô-đun bluetooth đầu tiên hoặc mô-đun wi-fi đầu tiên trong đó để truyền dữ liệu điều khiển để điều khiển phương tiện như một tín hiệu điều khiển phương tiện; bộ điều khiển từ xa trên xe được trang bị với mô-đun bluetooth thứ hai hoặc mô-đun wi-fi thứ hai để nhận tín hiệu điều khiển phương tiện.

Bản chất kỹ thuật của sáng chế

[Vấn đề kỹ thuật]

Sáng chế được đề xuất để giải quyết các vấn đề nêu trên bằng phương pháp thông thường, và mục tiêu của sáng chế là cung cấp một thiết bị mang chìa khóa điện tử, hệ thống và phương pháp, có khả năng điều khiển không dây và gửi quyền truy cập để điều khiển một hệ thống khóa, được cấu hình sao cho hoạt động của hệ thống khóa được điều khiển bằng các giao tiếp trong hệ thống và quyền điều khiển hệ thống khóa có thể được gán cho một chìa khóa điện tử khác thông qua một phương thức giao tiếp, mà nhờ đó,

đơn giản một chìa khóa điện tử có thể được gửi đi hoặc cho mượn tới một khoảng cách xa thông qua một mạng lưới liên lạc.

Ngoài ra, một mục tiêu khác của sáng chế là cung cấp một thiết bị mang chìa khóa điện tử, hệ thống và phương pháp liên quan đến chúng, có khả năng điều khiển không dây và gửi quyền truy cập để điều khiển hệ thống khóa, có thể được cài đặt gián tiếp bằng cách sử dụng các thiết bị thông minh phổ biến và việc xác thực người dùng có thể được thực hiện với một máy ảnh, màn hình, microphone, hoặc thiết bị tương tự đã được cài đặt sẵn trong các thiết bị thông minh đó, đồng thời giải quyết vấn đề sử dụng bất hợp pháp hoặc sao chép chìa khóa điện tử bằng cách tạo ra chìa khóa điện tử sử dụng một mã số phụ thuộc vào từng thiết bị.

Một mục tiêu khác của sáng chế là cung cấp một thiết bị mang chìa khóa điện tử, hệ thống và phương pháp liên quan đến chúng, có khả năng điều khiển không dây và gửi quyền truy cập để điều khiển hệ thống khóa, trong đó hệ thống chìa khóa điện tử được cấu hình bằng cách sử dụng một ứng dụng khóa điện tử được cài đặt trong một thiết bị thông minh, sao cho hoạt động của hệ thống khóa có thể bị giới hạn tùy thuộc vào một hoặc nhiều giá trị tham số đã cài đặt như thời gian, tọa độ GPS, nhiệt độ và độ ẩm, nhờ đó mà hoạt động của hệ thống khóa có thể được điều khiển một cách có giới hạn tùy thuộc vào thời gian, các khu vực (địa điểm), môi trường bên ngoài, hoặc các tham số tương tự, đồng thời các quyền truy cập khác nhau có thể được chỉ định.

[Giải pháp kỹ thuật]

Để đạt được các mục tiêu nói trên, thiết bị mang chìa khóa điện tử, theo các nội dung của điểm 1 yêu cầu bảo hộ được đề xuất.

Theo phương án ưu tiên, mô-đun giao tiếp thứ nhất có thể giao tiếp với hệ thống khóa sử dụng một hoặc nhiều phương thức giao tiếp được chọn từ nhóm gồm tia hồng ngoại, RFID, NFC và Bluetooth, và mô-đun giao tiếp thứ hai có thể giao tiếp với thiết bị mang chìa khóa điện tử bổ sung sử dụng Wi-Fi hoặc một mạng thông tin di động.

Theo phương án ưu tiên, mô-đun xác thực người dùng nhằm thực hiện việc xác

thực người dùng khi điều khiển hoạt động của hệ thống khóa hoặc khi gán quyền truy cập cho thiết bị mang chìa khóa điện tử bổ sung nhằm điều khiển hệ thống khóa đó có thể được cài đặt, trong đó việc xác thực người dùng có thể được thực hiện bằng cách sử dụng một hoặc nhiều phương thức như xác nhận trông mắt, nhận diện khuôn mặt, nhận dạng vân tay, nhận dạng giọng nói, mặt khẩu, hoặc mẫu hình.

Theo phương án ưu tiên, thiết bị mang chìa khóa điện tử có thể điều khiển hoạt động của hệ thống khóa dựa vào một hoặc nhiều giá trị tham số cài đặt trước được lựa chọn trong các tham số thời gian, tọa độ GPS, nhiệt độ và độ ẩm.

Theo phương án ưu tiên, thiết bị mang chìa khóa điện tử có thể là thiết bị thông minh, được cài sẵn ứng dụng chìa khóa điện tử của một chiếc xe, và có thể được cấu hình để điều khiển không dây hoạt động của một hệ thống khóa cài đặt trong xe và để gán quyền truy cập điều khiển hoạt động của hệ thống khóa, đến một thiết bị thông minh khác.

[Hiệu quả của sáng chế]

Đối với thiết bị mang chìa khóa điện tử, hệ thống chìa khóa điện tử và phương pháp tạo lập hệ thống chìa khóa điện tử có khả năng điều khiển không dây và gửi quyền truy cập để điều khiển một hệ thống khóa, được đề xuất trong sáng chế, hoạt động của hệ thống khóa được điều khiển bằng cách giao tiếp với nhau và quyền truy cập để điều khiển hệ thống khóa, có thể được gán cho một thiết bị mang chìa khóa điện tử khác bằng cách giao tiếp với nhau, nhờ đó chìa khóa điện tử có thể được gửi đi hoặc cho mượn một cách đơn giản trên một khoảng cách dài thông qua mạng lưới thông tin liên lạc.

Ngoài ra, theo sáng chế, việc cài đặt chìa khóa điện tử có thể được thực hiện một cách đơn giản và tiết kiệm chi phí, việc xác thực người dùng được thực hiện bằng cách sử dụng máy ảnh, màn hình, microphone, hoặc thiết bị tương tự đã được cài đặt trong các thiết bị thông minh, và chìa khóa điện tử được tạo bằng cách sử dụng một mã số phụ

thuộc vào từng thiết bị, theo đó giải quyết được tình trạng sử dụng bất hợp pháp hay sao chép chìa khóa điện tử.

Hơn nữa, theo sáng chế, bằng cách sử dụng ứng dụng chìa khóa điện tử được cài đặt trong một thiết bị thông minh, hoạt động của hệ thống khóa có thể được giới hạn theo một hoặc nhiều giá trị tham số định sẵn được lựa từ các tham số về thời gian, tọa độ GPS, nhiệt độ và độ ẩm, nhờ đó hoạt động của hệ thống khóa có thể được hạn chế theo thời gian, địa điểm, môi trường bên ngoài, hoặc các tham số tương tự, và các quyền truy cập khác nhau có thể được chỉ định.

Mô tả vắn tắt hình vẽ

Fig.1 là hình vẽ minh họa thiết bị mang chìa khóa điện tử có khả năng điều khiển không dây và gửi quyền truy cập để điều khiển hệ thống khóa theo một phương án của sáng chế;

Fig.2 là hình vẽ minh họa quy trình điều khiển không dây và gửi quyền truy cập để điều khiển hệ thống khóa của thiết bị mang chìa khóa điện tử theo một phương án của sáng chế;

Fig.3 là hình vẽ minh họa mô-đun xác thực người dùng của thiết bị mang chìa khóa điện tử có khả năng điều khiển không dây và gửi quyền truy cập để điều khiển hệ thống khóa, theo một phương án của sáng chế;

Fig.4 là hình vẽ minh họa một ví dụ về hạn chế hoạt động của hệ thống khóa trong thiết bị mang chìa khóa điện tử có khả năng điều khiển không dây và gửi quyền truy cập để điều khiển hệ thống khóa theo một phương án của sáng chế;

Fig.5 là hình vẽ minh họa hệ thống chìa khóa điện tử có khả năng điều khiển không dây và gửi quyền truy cập để điều khiển hệ thống khóa theo một phương án của sáng chế;

Fig.6 là hình vẽ minh họa lưu đồ của phương pháp điều khiển không dây và gửi quyền truy cập để điều khiển hệ thống khóa bằng cách sử dụng chìa khóa điện tử theo

một phương án của sáng chế;

Fig.7 là hình vẽ minh họa lưu đồ của phương pháp điều khiển không dây và gửi quyền truy cập để điều khiển hệ thống khóa bằng cách sử dụng chìa khóa điện tử theo một phương án khác của sáng chế;

Fig.8 là hình vẽ minh họa một ví dụ về việc tạo lập và sử dụng chìa khóa điện tử trong pháp điều khiển không dây và gửi quyền truy cập để điều khiển hệ thống khóa bằng cách sử dụng chìa khóa điện tử theo một phương án của sáng chế.

(Mô tả chữ số tham chiếu trong các hình vẽ)

10: Hệ thống khóa

20: Thiết bị mang chìa khóa điện tử (Thiết bị mang chìa khóa chính)

30: Thiết bị mang chìa khóa điện tử (Thiết bị mang chìa khóa phụ)

100, 100': Mô-đun giao tiếp thứ nhất

200, 200': Mô-đun giao tiếp thứ hai

300, 300': Mô-đun điều khiển

310: Bộ phận tạo lập chìa khóa điện tử

320: Bộ phận điều khiển hệ thống khóa

330: Bộ phận truyền dẫn quyền điều khiển

400: Mô-đun xác thực người dùng

S100: Một bước trong đó thiết bị thông minh thứ nhất có cài đặt một ứng dụng chìa khóa điện tử, tạo lập một chìa khóa chính tương ứng với hệ thống khóa

S100': Một bước trong đó thiết bị thông minh thứ nhất có cài đặt một ứng dụng chìa khóa điện tử, tạo lập một chìa khóa chính tương ứng với một hệ thống khóa, đồng thời chìa khóa chính có chứa một mã số phụ thuộc vào thiết bị thông minh thứ nhất

S200: Một bước trong đó chìa khóa chính được tạo lập ở bước S100 được lưu trữ

trong thiết bị thông minh thứ nhất và đăng ký trong hệ thống khoá

S300: Một bước trong đó thiết bị thông minh thứ nhất mang chìa khóa chính tạo lập một chìa khóa phụ để điều khiển hoạt động của hệ thống khóa trong một phạm vi định sẵn và gửi chìa khóa phụ tới thiết bị thông minh thứ hai có cài đặt sẵn ứng dụng chìa khóa điện tử, nhờ đó quyền truy cập để điều khiển hệ thống khóa được gán cho thiết bị thông minh thứ hai.

S300': Một bước trong đó thiết bị thông minh thứ nhất có lưu trữ chìa khóa chính, tạo lập một chìa khóa phụ, mang các mã số phụ thuộc vào thiết bị thông minh thứ nhất và thứ hai, để điều khiển hoạt động của hệ thống khóa trong một phạm vi định sẵn, và gửi chìa khóa phụ tới thiết bị thông minh thứ hai có cài đặt sẵn ứng dụng chìa khóa điện tử, theo đó quyền truy cập để điều khiển hệ thống khóa được gán cho thiết bị thông minh thứ hai.

S310: Một bước trong đó chìa khóa phụ, gửi trong bước S300', được lưu trữ trong thiết bị thông minh thứ hai và đăng ký trong hệ thống khoá.

S400: là bước trong đó thiết bị thông minh thứ nhất hoặc thiết bị thông minh thứ hai điều khiển hoạt động của hệ thống khóa bằng cách gửi tín hiệu điều khiển hoạt động cho hệ thống khóa

S400': Là bước trong đó thiết bị thông minh thứ nhất hoặc thiết bị thông minh thứ hai điều khiển hoạt động của hệ thống khóa bằng cách gửi tín hiệu điều khiển hoạt động và tín hiệu tương ứng với chìa khóa chính và chìa khóa phụ mang các mã số của thiết bị thông minh thứ nhất hoặc thiết bị thông minh thứ hai, tới hệ thống khóa.

Mô tả chi tiết sáng chế

Phương án ưu tiên của sáng chế được mô tả dưới đây tham chiếu tới các hình vẽ đi kèm nhằm mô tả sáng chế một cách chi tiết đến mức những người có hiểu biết trung bình về lĩnh vực kỹ thuật của sáng chế có thể dễ dàng thực hiện. Trong phần mô tả dưới đây, cần lưu ý rằng, khi các chức năng của các bộ phận thông thường và các mô tả chi

tiết về các bộ phận có liên quan với sáng chế có thể làm cho các nội dung cơ bản của sáng chế không rõ ràng, thì phần mô tả chi tiết của những bộ phận đó sẽ bị loại bỏ. Ngoài ra, cần tham chiếu tới các hình vẽ trong đó các số tham chiếu được sử dụng đồng nhất trong các hình vẽ khác nhau nhằm đề cập tới các bộ phận giống nhau hoặc tương tự nhau.

Hơn nữa, trong suốt toàn bộ nội dung bản mô tả này, khi diễn giải rằng bộ phận thứ nhất “kết nối” với bộ phận thứ hai thì cần được hiểu rằng việc kết nối đó sẽ bao gồm trường hợp bộ phận thứ nhất được “kết nối gián tiếp” với bộ phận thứ hai thông qua các thiết bị trung gian khác, và trường hợp bộ phận thứ nhất được “kết nối trực tiếp” với bộ phận thứ hai. Cụ thể hơn, khi diễn giải rằng bộ phận thứ nhất “bao gồm” bộ phận thứ hai thì có nghĩa là có thể còn bao gồm các bộ phận khác, không loại trừ khả năng các bộ phận khác sẽ được bổ sung, trừ trường hợp được mô tả ngược lại trong một bối cảnh cụ thể.

Fig.1 là hình vẽ minh họa thiết bị mang chìa khóa điện tử có khả năng điều khiển không dây và gửi quyền truy cập để điều khiển hệ thống khóa theo một phương án của sáng chế.

Như minh họa ở Fig.1, thiết bị mang chìa khóa điện tử 20 có khả năng điều khiển không dây và gửi quyền truy cập để điều khiển hệ thống khóa theo một phương án của sáng chế là thiết bị dùng để điều khiển hoạt động của hệ thống khóa 10 bằng cách giao tiếp với hệ thống khóa 10, và được cấu hình để bao gồm mô-đun giao tiếp thứ nhất 100, mô-đun giao tiếp thứ hai 200, và mô-đun điều khiển 300.

Theo phương án ưu tiên, thiết bị mang chìa khóa điện tử có khả năng điều khiển không dây và gửi quyền truy cập để điều khiển hệ thống khóa theo một phương án của sáng chế, có thể là thiết bị thông minh trong đó ứng dụng chìa khóa điện tử đã được cài đặt sẵn. Thiết bị thông minh là sản phẩm được cấu hình sao cho các chức năng của nó không bị giới hạn và hầu hết các chức năng đó có thể được thay đổi hoặc được mở rộng thông qua các chương trình ứng dụng, và theo đó, một chiếc điện thoại thông minh có thể tải xuống và cài đặt các ứng dụng (phần mềm) chính là một ví dụ điển hình của thiết bị thông minh nêu trên. Tuy nhiên, không giới hạn bởi thiết bị nêu trên, bất kỳ thiết bị

nào mà có thể được cài đặt được ứng dụng chìa khóa điện tử, chẳng hạn như iPad, máy tính bảng, hoặc thiết bị tương tự, đều có thể đóng vai trò của chìa khóa điện tử theo nội dung của sáng chế, bất kể hình dạng cụ thể của thiết bị đầu cuối. Mặc dù vậy, theo sáng chế, bởi vì điều quan trọng là việc cung cấp cho người sử dụng một thiết bị di động có thể hoạt động như một chìa khóa, nên tốt nhất là sử dụng chiếc điện thoại thông minh mà một người bình thường có thể dễ dàng và cần thiết để mang theo.

Theo một phương án của sáng chế, thiết bị mang chìa khóa điện tử 20 có thể là một thiết bị thông minh trong đó ứng dụng chìa khóa điện tử cho một chiếc xe được cài đặt, và có thể điều khiển không dây hoạt động của hệ thống khóa 10 cài đặt trong xe và gán quyền truy cập để điều khiển hệ thống khóa cho thiết bị thông minh 30 khác. Tuy nhiên, đây cũng chỉ là một phương án cụ thể của sáng chế, và thiết bị mang chìa khóa điện tử không chỉ dùng cho một chiếc xe mà còn có thể được ứng dụng cho nhiều thiết bị cơ khí khác có yêu cầu quyền truy cập của người sử dụng, như là các loại khóa cửa.

Mô-đun giao tiếp thứ nhất 100 dùng để giao tiếp với hệ thống khóa 10, và có thể thông qua một hoặc nhiều phương thức giao tiếp được lựa chọn như tia hồng ngoại, RFID, NFC và Bluetooth. Mô-đun giao tiếp thứ hai 200 dùng để giao tiếp với chìa khóa điện tử phụ 30, và có thể sử dụng Wi-Fi hoặc mạng thông tin di động.

Mô-đun điều khiển 300 được cấu hình để bao gồm bộ phận tạo lập chìa khóa điện tử 310 nhằm tạo ra chìa khóa điện tử tương ứng với hệ thống khóa 10, bộ phận điều khiển hệ thống khóa 320 để đăng ký chìa khóa điện tử tương ứng với hệ thống khóa 10 thông qua mô-đun giao tiếp 100, và bộ phận truyền dẫn quyền điều khiển 330 để gán quyền truy cập để điều khiển hệ thống khóa cho chìa khóa điện tử phụ 30 thông qua mô-đun giao tiếp thứ hai 200.

Fig.2 là hình vẽ minh họa quá trình trong đó thiết bị mang chìa khóa điện tử thực hiện việc điều khiển không dây và gửi quyền truy cập để điều khiển hệ thống khóa theo một phương án của sáng chế. Như minh họa ở Fig.2, khi chìa khóa điện tử tương ứng với hệ thống khóa 10 được tạo ra trong thiết bị mang chìa khóa điện tử 20 có khả năng điều khiển không dây và gửi quyền truy cập để điều khiển hệ thống khóa, được đề xuất trong sáng chế, thì chìa khóa điện tử đó cũng được đăng ký với hệ thống khóa 10 như

một người dùng chính thức và được phép truy cập vào hệ thống khóa. Ngoài ra, thiết bị mang chìa khóa điện tử 20 có chứa chìa khóa điện tử đã đăng ký, có thể điều khiển hoạt động của hệ thống khóa 10 thông qua mô-đun giao tiếp thứ nhất 100. Trong khi đó, thiết bị mang chìa khóa điện tử 20, được đề xuất trong sáng chế, không những chỉ có chức năng điều khiển không dây hệ thống khóa 10 mà còn có chức năng gán quyền truy cập cho thiết bị mang chìa khóa điện tử phụ 30 cho phép thiết bị mang chìa khóa điện tử bổ sung này điều khiển hệ thống khóa trong một phạm vi nhất định.

Phương pháp gán quyền truy cập để điều khiển hệ thống khóa, có thể được cấu hình sao cho thiết bị mang chìa khóa điện tử 20 có thể tự tạo ra một chìa khóa điện tử mới (chìa khóa phụ kèm theo) để cài đặt trong một thiết bị mang chìa khóa điện tử phụ 30, bằng cách sử dụng ứng dụng để tạo lập chìa khóa điện tử, sau đó sẽ gửi chìa khóa mới được tạo lập này tới thiết bị mang chìa khóa điện tử phụ 30. Tuy nhiên, đây cũng chỉ là một phương án cụ thể của sáng chế, và quy trình gán quyền điều khiển hoạt động có thể được thực hiện thông qua một máy chủ cung cấp dịch vụ. Trong khi đó, khi chìa khóa điện tử được tạo lập và sử dụng, việc tạo ra một chỉ số nhận dạng (ID) được mã hóa, một mã được trích xuất từ đó, và một mã số được tạo lập ngẫu nhiên một lần nhận được từ hệ thống khóa có thể được sử dụng. Nội dung này sẽ được mô tả cụ thể tại Fig.8. Sáng chế cung cấp một thiết bị mang chìa khóa điện tử có chức năng truyền tải không dây quyền truy cập để điều khiển hệ thống khóa mà nhờ đó chìa khóa điện tử đơn giản có thể được gửi hoặc cho mượn trên một khoảng cách dài thông qua mạng lưới thông tin liên lạc.

Fig.3 là hình vẽ minh họa mô-đun xác thực người dùng của thiết bị mang chìa khóa điện tử có khả năng điều khiển không dây và gửi quyền truy cập để điều khiển hệ thống khóa theo một phương án của sáng chế. Như minh họa ở Fig.3, thiết bị mang chìa khóa điện tử 20 có khả năng điều khiển không dây và gửi quyền truy cập để điều khiển hệ thống khóa theo một phương án của sáng chế có thể bao gồm mô-đun xác thực người dùng 400. Tại đây, mô-đun xác thực người dùng 400 làm nhiệm vụ xác thực người dùng khi điều khiển hoạt động của hệ thống khóa 10 hoặc khi gán quyền truy cập cho thiết bị mang chìa khóa điện tử phụ 30. Xác thực người dùng có thể được thực hiện thông qua

một hoặc nhiều lựa chọn trong số các phương thức nhận dạng như: nhận dạng trông mắt, nhận diện khuôn mặt, nhận dạng vân tay, nhận dạng giọng nói, mặt khẩu, và mẫu hình. Tuy nhiên, có nhiều biến thể khác nhau của thiết bị, và việc xác thực người dùng là không giới hạn đối với các biến thể này. Khi thiết bị thông minh, đã được cấu hình sẵn với máy ảnh, màn hình, micro, và các thiết bị tương tự, được sử dụng như là thiết bị mang chìa khóa điện tử 20 thì việc xác thực người dùng có thể được thực hiện bằng cách sử dụng các thiết bị này. Do thiết bị mang chìa khóa điện tử 20 được đề xuất trong sáng chế được cấu hình để tạo ra chìa khóa điện tử được mã hóa trong một giải pháp phần mềm, để chuyển đổi chìa khóa điện tử thành tín hiệu, và gửi các tín hiệu đó đi, thuận lợi của giải pháp này là chìa khóa điện tử có thể được gửi đi, thay thế, hoặc cho mượn một cách đơn giản, nhưng bất lợi là ở chỗ chìa khóa điện tử rất dễ bị sử dụng bất hợp pháp hoặc sao chép, nhân bản. Tuy vậy, mô-đun xác thực người dùng 400 có thể giúp chìa khóa điện tử được kiểm soát chỉ bởi một người dùng nhất định qua đó giải quyết được vấn đề sử dụng chìa khóa điện tử bất hợp pháp hoặc sao chép, nhân bản chìa khóa điện tử.

Fig.4 là hình vẽ minh họa một ví dụ về điều khiển hạn chế của hệ thống khóa trong thiết bị mang chìa khóa điện tử có khả năng điều khiển không dây và gửi quyền truy cập để điều khiển hệ thống khóa theo một phương án của sáng chế. Như minh họa ở Fig.4, thiết bị mang chìa khóa điện tử 20 theo một phương án của sáng chế và thiết bị mang chìa khóa điện tử phụ 30, sau khi nhận được quyền truy cập để điều khiển hệ thống khóa từ thiết bị mang chìa khóa điện tử 20, độc lập điều khiển hoạt động của hệ thống khóa 10, nhưng có thể điều khiển hoạt động của hệ thống khóa 10 phụ thuộc vào một hoặc nhiều giá trị trong số tham số đã được lựa chọn trước và cài đặt trước như thời gian, trị tọa độ GPS, nhiệt độ và độ ẩm. Như đã mô tả ở trên với tham chiếu đến Fig.3, vì thiết bị mang chìa khóa điện tử 20 rất dễ bị sử dụng bất hợp pháp hay bị sao chép nhân bản, vì vậy quyền điều khiển có thể được giới hạn. Cụ thể, việc điều khiển hoạt động của hệ thống khóa 10 có thể được cài đặt sử dụng theo ngày, giờ hoặc một khoảng thời gian xác định, hoặc theo một khu vực địa lý nhất định bằng cách sử dụng thiết bị định vị GPS kèm theo thiết bị mang chìa khóa điện tử 20 hoặc hệ thống khóa 10. Hơn

nữa, quyền điều khiển còn có thể được giới hạn theo môi trường bên ngoài như nhiệt độ, độ ẩm, hoặc các thông số tương tự. Những giới hạn có thể được cài đặt trước trong thiết bị mang chìa khóa điện tử 20, hoặc thiết bị mang chìa khóa điện tử 20 có thể gán quyền truy cập hạn chế để điều khiển hệ thống khóa cho thiết bị mang chìa khóa điện tử phụ 30. Cụ thể, khi các quyền truy cập được gán cho thiết bị mang chìa khóa điện tử phụ 30, thì chức năng gán quyền truy cập hạn chế có thể được cài đặt sao cho việc lái xe được quản lý tạm thời với hạn chế về thời gian, hoặc việc sử dụng chiếc xe chỉ được cho phép trong một khu vực địa lý hoặc một môi trường xác định khi chiếc xe đó được cho một người bạn mượn.

Fig.5 là hình vẽ minh họa hệ thống chìa khóa điện tử có khả năng điều khiển không dây và gửi quyền truy cập để điều khiển hệ thống khóa theo một phương án của sáng chế. Như minh họa ở Fig.5, hệ thống chìa khóa điện tử có khả năng điều khiển không dây và gửi quyền truy cập để điều khiển hệ thống khóa theo một phương án của sáng chế có thể được cấu hình để bao gồm thiết bị mang chìa khóa chính 20, nhằm điều khiển hoạt động của hệ thống khóa 10 bằng cách giao tiếp với hệ thống khóa 10 và gán quyền truy cập để điều khiển hệ thống khóa cho thiết bị mang chìa khóa điện tử phụ 30 bằng cách giao tiếp với chính thiết bị mang chìa khóa điện tử phụ 30, và thiết bị mang chìa khóa phụ 30, để tiếp nhận quyền điều khiển hệ thống khóa từ thiết bị mang chìa khóa chính 20 và để điều khiển hoạt động của hệ thống khóa 10 trong phạm vi đã được giới hạn. Thiết bị mang chìa khóa chính 20 được đề xuất trong sáng chế và được mô tả tham chiếu từ Fig.1 đến Fig.4 chính là thiết bị mang chìa khóa điện tử có khả năng điều khiển không dây và gửi quyền truy cập để điều khiển hệ thống khóa, và thiết bị mang chìa khóa phụ 30 cũng chính là thiết bị mang chìa khóa điện tử bổ sung, có khả năng nhận quyền truy cập để điều khiển hệ thống khóa 10 từ thiết bị mang chìa khóa điện tử chính có khả năng điều khiển không dây và gửi quyền truy cập để điều khiển hệ thống khóa. Thiết bị mang chìa khóa chính và thiết bị mang chìa khóa phụ có thể là thiết bị thông minh trong đó một ứng dụng chìa khóa điện tử đã được cài đặt. Thiết bị mang chìa khóa phụ 30 cũng có thể bao gồm một mô-đun giao tiếp thứ nhất 100' để giao tiếp với hệ thống khóa 10, và mô-đun giao tiếp thứ hai 200' để giao tiếp với thiết bị mang

chìa khóa chính 20, và mô-đun điều khiển 300' để điều khiển các mô-đun giao tiếp.

Fig. 6 là hình vẽ minh họa lưu trình của phương pháp điều khiển không dây và gửi quyền truy cập để điều khiển một hệ thống khóa theo một phương án của sáng chế. Như minh họa ở Fig.6, phương pháp điều khiển không dây và gửi quyền truy cập để điều khiển hệ thống khóa theo một phương án của sáng chế là có thể được thực hiện để bao gồm Bước (S100), trong đó thiết bị thông minh thứ nhất đã được cài đặt sẵn ứng dụng chìa khóa điện tử, sẽ tạo lập chìa khóa chính tương ứng với hệ thống khóa, bước (S200), là chìa khóa chính được tạo ra ở bước S100 sẽ được lưu trữ trong thiết bị thông minh thứ nhất và được đăng ký với hệ thống khóa, bước (S300), trong đó thiết bị thông minh thứ nhất mang chìa khóa chính sẽ gán quyền truy cập để điều khiển hệ thống khóa cho thiết bị thông minh thứ hai bằng cách tạo ra chìa khóa để điều khiển hoạt động của hệ thống khóa trong một phạm vi định sẵn và gửi chìa khóa phụ đó tới thiết bị thông minh thứ hai đã được cài đặt sẵn ứng dụng khóa điện tử, và bước (S400) là quá trình thiết bị thông minh thứ nhất hoặc thiết bị thông minh thứ hai thực hiện việc điều khiển hoạt động của hệ thống khóa bằng cách gửi tín hiệu điều khiển hoạt động tới hệ thống khóa đó.

Cụ thể là, người sử dụng có thể đọc các điều kiện hạn chế hoạt động của hệ thống khóa đã được cài đặt trước bằng cách sử dụng một giao thức tương tác không dây giữa thiết bị thông minh thứ nhất và hệ thống khóa, và có thể nhập các giá trị tham số điều kiện cần thiết cho hạn chế hoạt động hệ thống khóa, thông qua thiết bị thông minh thứ nhất khi tạo lập chìa khóa chính. Ở đây, chìa khóa chính có thể được tạo lập để bao gồm một chỉ số nhận dạng (ID) phụ thuộc vào thiết bị thông minh thứ nhất, các giá trị tham số đầu vào điều kiện hạn chế điều khiển hệ thống khóa, thông tin về các giá trị tham số cần thiết để tạo lập chìa khóa phụ, và thông tin xác thực người dùng theo cấp độ bảo mật, đồng thời chìa khóa chính sẽ lưu trữ trong thiết bị thông minh thứ nhất và được đăng ký với hệ thống khóa. Hệ thống chìa khóa điện tử có thể được cho phép giao tiếp với hệ thống khóa chỉ trong khoảng cách ngắn thông qua như giao thức không dây trong phạm vi gần được mã hóa (NFC, Bluetooth, tia hồng ngoại, hoặc tương tự), quy trình bảo mật có thể được cài đặt để kiểm tra mật khẩu, mẫu hình, sinh trắc học, hoặc các

điều kiện tương tự tùy thuộc vào mức độ bảo mật đã thiết lập, và quy trình xác thực chủ sở hữu của thiết bị thông minh thứ hai có thể được thực hiện bằng sinh trắc học hoặc giải pháp tương tự ở thiết bị thông minh thứ hai như ở thiết bị thông minh thứ nhất.

Chìa khóa phụ của thiết bị thông minh thứ hai có thể bao gồm chỉ số nhận dạng (ID) phụ thuộc thiết bị thông minh thứ nhất, chỉ số nhận dạng (ID) phụ thuộc thiết bị thông minh thứ hai, mật khẩu (và/hoặc sinh trắc học), và các thông tin về giá trị tham số giới hạn (thông tin định vị GPS, thời gian tạo lập, thời gian hết hạn, và tham số tương tự). Chìa khóa điện tử (chìa khóa chính hoặc chìa khóa phụ) có thể được tạo lập trong thiết bị thông minh thứ nhất hoặc thiết bị thông minh thứ hai thông qua thủ tục xác thực bằng cách sử dụng điện thoại di động, và chìa khóa phụ có thể được chuyển bằng Wi-Fi hoặc mạng thông tin di động (3G, 4G, LTE, hoặc tương tự). Thiết bị thông minh thứ hai có thể bao gồm nhiều thiết bị, và thiết bị thông minh thứ hai này mang chìa khóa phụ đã được tạo lập, có thể được phép điều khiển hoạt động của hệ thống khóa chỉ bằng cách thực hiện quy trình xác thực người dùng tùy thuộc vào mức độ bảo mật đã thiết lập.

Hệ thống khóa có thể được cấu hình sao cho một hoặc nhiều mô-đun giao tiếp không dây trong phạm vi gần (NFC, Bluetooth, tia hồng ngoại, RFID, hoặc tương tự) được cài đặt trong đó để giao tiếp với thiết bị thông minh thứ nhất hoặc thứ hai, đồng thời cũng có thể bao gồm một mô-đun mạch điện tử chỉ được phép mở cho người sử dụng có quyền truy cập và hệ thống khóa theo cấp độ bảo mật. Hệ thống khóa tự nó có thể bao gồm chức năng cài đặt giờ và chức năng khóa tự động để cho phép chìa khóa điện tử điều khiển hệ thống khóa chỉ trong một khoảng thời gian nhất định. Hệ thống khóa theo một phương án của sáng chế có thể được sản xuất dưới dạng một mô-đun cho một thiết bị cụ thể hoặc dưới dạng một mô-đun tương thích với các loại thiết bị khác nhau, chẳng hạn như bán dẫn ASIC, bộ nhớ di động USB, bản mạch cho khe khóa, hoặc tương tự.

Fig.7 là hình vẽ minh họa lưu trình của phương pháp điều khiển không dây và gửi quyền truy cập để điều khiển hệ thống khóa theo một phương án của sáng chế. Như minh họa ở Fig.7, phương pháp theo một phương án khác của sáng chế có thể được thực hiện để bao gồm bước (S100'), trong đó thiết bị thông minh thứ nhất có cài đặt ứng

dụng chìa khóa điện tử, tạo lập một chìa khóa chính tương ứng với hệ thống khóa và mang chỉ số nhận dạng (ID) phụ thuộc thiết bị thông minh thứ nhất, bước (S200), trong đó chìa khóa chính đã được tạo lập ở bước S100 được lưu trữ trong thiết bị thông minh thứ nhất và được đăng ký với hệ thống khóa, bước (S300), trong đó thiết bị thông minh thứ nhất 100 mang chìa khóa chính, sẽ tạo lập chìa khóa phụ để điều khiển hoạt động của hệ thống khóa trong một phạm vi được cài đặt trước, chìa khóa phụ này cũng mang chỉ số nhận dạng (ID) phụ thuộc vào thiết bị thông minh thứ nhất và thiết bị thông minh thứ hai, sau đó gửi chìa khóa phụ mới được tạo lập tới thiết bị thông minh thứ hai đã được cài đặt sẵn ứng dụng chìa khóa điện tử mà theo đó quyền truy cập để điều khiển hệ thống khóa được gán cho thiết bị thông minh thứ hai, bước (S310), trong đó chìa khóa phụ mới được gửi tới sẽ được lưu trữ trong thiết bị thông minh thứ hai và được đăng ký với hệ thống khóa, và bước (S400'), trong đó thiết bị thông minh thứ nhất hoặc thiết bị thông minh thứ hai điều khiển hoạt động của hệ thống khóa bằng cách gửi tín hiệu điều khiển hoạt động của hệ thống khóa và tín hiệu tương ứng với chìa khóa chính hoặc chìa khóa phụ mang chỉ số nhận dạng (ID) của các thiết bị thông minh thứ nhất hoặc thiết bị thông minh thứ hai, tới hệ thống khóa. Nói cách khác, chìa khóa chính được cấu hình để bao gồm chỉ số nhận dạng (ID) phụ thuộc thiết bị thông minh thứ nhất, và chìa khóa phụ cũng được cấu hình để bao gồm chỉ số nhận dạng (ID) phụ thuộc vào thiết bị thông minh thứ nhất và thiết bị thông minh thứ hai, và hệ thống khóa có thể nhận tín hiệu tương ứng với chìa khóa chính hoặc chìa khóa phụ mang chỉ số nhận dạng (ID) của thiết bị thông minh thứ nhất hoặc thiết bị thông minh thứ hai, từ thiết bị thông minh thứ nhất hoặc thiết bị thông minh thứ hai, đồng thời có thể cho phép truy cập vào quyền điều khiển nếu chỉ số nhận dạng (ID) nhận được khớp với chỉ số nhận dạng (ID) đã được đăng ký trước đó. Ngoài ra, để nâng cao mức độ bảo mật, phương pháp này có thể được thực hiện sao cho quyền truy cập chỉ mở khi thiết bị thông minh thứ hai được đăng ký với hệ thống khóa thông qua phương thức giao tiếp phạm vi gần sau bước S300'.

Fig.8 là hình vẽ minh họa một ví dụ trong đó chìa khóa điện tử được tạo lập và sử dụng trong phương pháp điều khiển không dây và gửi quyền truy cập để điều khiển hệ thống khóa theo một phương án của sáng chế. Như minh họa ở Fig.8, chìa khóa điện tử

có thể được cấu hình để mang một chỉ số nhận dạng (ID) duy nhất được tạo ra trên một thiết bị duy nhất. Nói cách khác, chỉ số nhận dạng (ID) được cấu hình để bao gồm số sê-ri, địa chỉ MAC (mã duy nhất được gán bởi nhà sản xuất), và chỉ số nhận dạng (ID) mô-đun của thiết bị tương ứng, theo đó chỉ số nhận dạng (ID) phụ thuộc vào thiết bị mang chìa khóa điện tử tương ứng (thiết bị thông minh thứ nhất) có thể được tạo lập và cài đặt trong chìa khóa điện tử. Theo một phương án, chìa khóa điện tử này cũng có thể được cấu hình để bao gồm thêm thông tin xác thực người dùng, các giá trị tham số, và thông tin tương tự. Khi thiết bị mang chìa khóa điện tử (thiết bị thông minh thứ nhất hoặc thiết bị thông minh thứ hai) truyền một tín hiệu truy cập vào hệ thống khóa, hệ thống khóa sẽ so sánh Chỉ số nhận dạng (ID) đã nhận của thiết bị với chỉ số nhận dạng (ID) đã được cài đặt trước. Nếu hai chỉ số nhận dạng (ID) đó khớp nhau, hệ thống khóa cho phép truy cập và điều khiển.

Theo một phương án của sáng chế, khi thiết bị thông minh thứ hai mã hóa chỉ số nhận dạng (ID) phụ thuộc thiết bị đã được đăng ký với hệ thống khóa, và truyền chỉ số nhận dạng (ID) đó qua giao tiếp trong phạm vi gần, hệ thống khóa sẽ so sánh chỉ số nhận dạng (ID) mới tiếp nhận với chỉ số nhận dạng (ID) đã được cài đặt trước đó. Nếu hai chỉ số nhận dạng (ID) này khớp nhau, hệ thống khóa sẽ gửi một tham số ngẫu nhiên và duy nhất, được tạo ra bởi một thiết bị tạo số ngẫu nhiên, đến thiết bị (thiết bị thông minh thứ hai) để yêu cầu xác thực thông qua giao tiếp không dây trong phạm vi gần. Sau đó, thiết bị thông minh thứ hai sẽ mã hóa mã số được lấy từ chỉ số nhận dạng (ID) duy nhất, sử dụng tham số ngẫu nhiên duy nhất đã được tiếp nhận, và truyền mã số đã được mã hóa tới hệ thống khóa qua mạng không dây. Ở đây, mã số được lấy có thể là mã được tạo thành từ một dãy số có độ dài nhất định bắt đầu từ một vị trí tùy ý theo thứ tự tăng dần hoặc giảm dần tính từ chỉ số nhận dạng (ID) phụ thuộc thiết bị. Hệ thống khóa sẽ kiểm tra, thông qua một mã đã tiếp nhận qua mạng không dây được lấy từ chỉ số nhận dạng (ID), xem thiết bị đó có phải là một điện thoại di động được cho phép sử dụng, đồng thời có thể nhận được các giá trị tham số còn lại bằng cách gửi lại lần nữa “số ngẫu nhiên một lần” (one-time random number). Các quyền truy cập được thiết lập dựa trên các giá trị tham số đã tiếp nhận được có thể kích hoạt tính năng điều khiển hệ

thống khóa. Phương pháp gửi một số đã được mã hóa sử dụng “số ngẫu nhiên một lần” tạo ra bởi thiết bị tạo số ngẫu nhiên và phương pháp sử dụng một số mã được lấy từ một chỉ số nhận dạng (ID) phụ thuộc thiết bị (có nghĩa là, sử dụng một chỉ số nhận dạng (ID) phụ thuộc thiết bị như một bảng số ngẫu nhiên) có thể ngăn ngừa việc lấy trộm các gói dữ liệu và sử dụng bất hợp pháp gói dữ liệu đó, theo đó, chỉ thiết bị được cho phép mới có thể điều khiển hệ thống khóa qua đó nâng cao được tính bảo mật.

Sáng chế nêu trên có thể được thay đổi hoặc được áp dụng theo nhiều cách bởi những người có hiểu biết trung bình về lĩnh vực kỹ thuật của sáng chế, và phạm vi của khái niệm kỹ thuật theo sáng chế phải được xác định bởi các yêu cầu bảo hộ sau đây.

YÊU CẦU BẢO HỘ

1. Thiết bị mang chìa khóa điện tử để điều khiển hoạt động của hệ thống khóa (10), thiết bị mang chìa khóa điện tử bao gồm thiết bị mang chìa khóa điện tử chính (20) và thiết bị mang chìa khóa điện tử phụ (30), thiết bị mang chìa khóa điện tử (20) có khả năng điều khiển không dây hệ thống khóa (10) và gửi quyền truy cập để điều khiển hệ thống khóa (10), bao gồm:

mô-đun giao tiếp thứ nhất (100) để giao tiếp với hệ thống khóa (10);

mô-đun giao tiếp thứ hai (200) để giao tiếp với thiết bị mang chìa khóa điện tử phụ (30);

mô-đun xác thực người dùng thứ nhất (400) để thực hiện việc xác thực thông tin người dùng khi điều khiển hoạt động của hệ thống khóa (10) hoặc khi gán quyền điều khiển hệ thống khóa (10) cho thiết bị mang chìa khóa điện tử phụ (30); và

mô-đun điều khiển thứ nhất (300) để điều khiển hoạt động của hệ thống khóa (10) thông qua mô-đun giao tiếp thứ nhất (100) và mô-đun giao tiếp thứ hai (200), trong đó

cụ thể trong đó thiết bị chìa khóa điện tử phụ (30) có khả năng điều khiển không dây hệ thống khóa (10) và nhận quyền truy cập từ thiết bị chìa khóa điện tử (20) để điều khiển hệ thống khóa (10), bao gồm:

mô-đun giao tiếp thứ ba (100') để giao tiếp với hệ thống khóa (10);

mô-đun giao tiếp thứ tư (200') để giao tiếp với thiết bị mang chìa khóa điện tử phụ (30);

mô-đun xác thực người dùng thứ hai (400) để thực hiện việc xác thực thông tin người dùng khi điều khiển hoạt động của hệ thống khóa (10) và

mô-đun điều khiển thứ hai (300') để điều khiển hoạt động của hệ thống khóa (10) thông qua mô-đun giao tiếp thứ ba (100') và mô-đun giao tiếp thứ tư (200'), trong đó mô-đun điều khiển thứ nhất (300) bao gồm:

bộ phận tạo lập chìa khóa điện tử (310) nhằm tạo ra chìa khóa điện tử tương ứng với hệ thống khóa (10);

bộ phận điều khiển hệ thống khóa (320) để đăng ký chìa khóa điện tử tương ứng với hệ thống khóa (10) thông qua mô-đun giao tiếp thứ nhất (100), và điều khiển hoạt động của hệ thống khóa (10) bằng cách gửi các tín hiệu hoạt động đến hệ thống khóa (10); và bộ phận truyền dẫn quyền điều khiển (330) để gán quyền truy cập để điều khiển hệ thống khóa (10) cho chìa khóa điện tử phụ (30) thông qua mô-đun giao tiếp thứ hai (200), và

trong đó mô-đun xác thực người dùng thứ nhất (400) được cấu hình để xác thực thiết bị mang chìa khóa điện tử chính (20) khi điều khiển hoạt động của hệ thống khóa (10) được thực hiện thông qua một trong các dấu hiệu nhận dạng như: nhận dạng trông mắt, nhận diện khuôn mặt, nhận dạng vân tay, nhận dạng giọng nói, mật khẩu, và mẫu hình được thực hiện bằng người dùng thứ nhất của thiết bị mang chìa khóa điện tử (20), và

mô-đun xác thực người dùng thứ hai (400) được cấu hình để xác thực thiết bị mang chìa khóa điện tử phụ (20) khi điều khiển hoạt động của hệ thống khóa (10) được thực hiện thông qua một trong các dấu hiệu nhận dạng trông mắt, nhận diện khuôn mặt, nhận dạng vân tay, nhận dạng giọng nói, mật khẩu, và mẫu hình được thực hiện bằng người dùng thứ hai của thiết bị mang chìa khóa điện tử phụ (30) và

và các quyền điều khiển được cấu hình để cho phép thiết bị mang chìa khóa điện tử phụ (30) chỉ thực hiện được việc điều khiển hoạt động của hệ thống khóa (10) duy tại một địa điểm xác định và trong một khoảng thời gian nhất định.

2. Thiết bị mang chìa khóa điện tử theo điểm 1, trong đó mô-đun giao tiếp thứ nhất (100) giao tiếp với hệ thống khóa (10) bằng cách sử dụng một hoặc nhiều phương thức được lựa chọn từ các phương thức như tia hồng ngoại, RFID, NFC và Bluetooth, và mô-đun giao tiếp thứ hai (200) giao tiếp với thiết bị mang chìa khóa điện tử phụ (30) thông qua Wi-Fi hoặc mạng thông tin di động.

3. Thiết bị mang chìa khóa điện tử theo điểm 1, trong đó thiết bị mang chìa khóa

điện tử điều khiển hoạt động của hệ thống khóa phụ thuộc vào các tham số được lựa chọn từ ít nhất một trong các giá trị về thời gian, tọa độ GPS, nhiệt độ và độ ẩm.

4. Thiết bị mang chìa khóa điện tử theo điểm 1, trong đó thiết bị mang chìa khóa điện tử (20) là thiết bị thông minh trong đó một ứng dụng chìa khóa điện tử cho một chiếc xe đã được cài đặt, và được cấu hình để điều khiển không dây hoạt động của hệ thống khóa (10) đã được cài đặt trong xe và gán quyền truy cập để điều khiển hoạt động của hệ thống khóa (10) đến thiết bị chìa khóa điện tử phụ như một thiết bị thông minh khác.

FIG.1

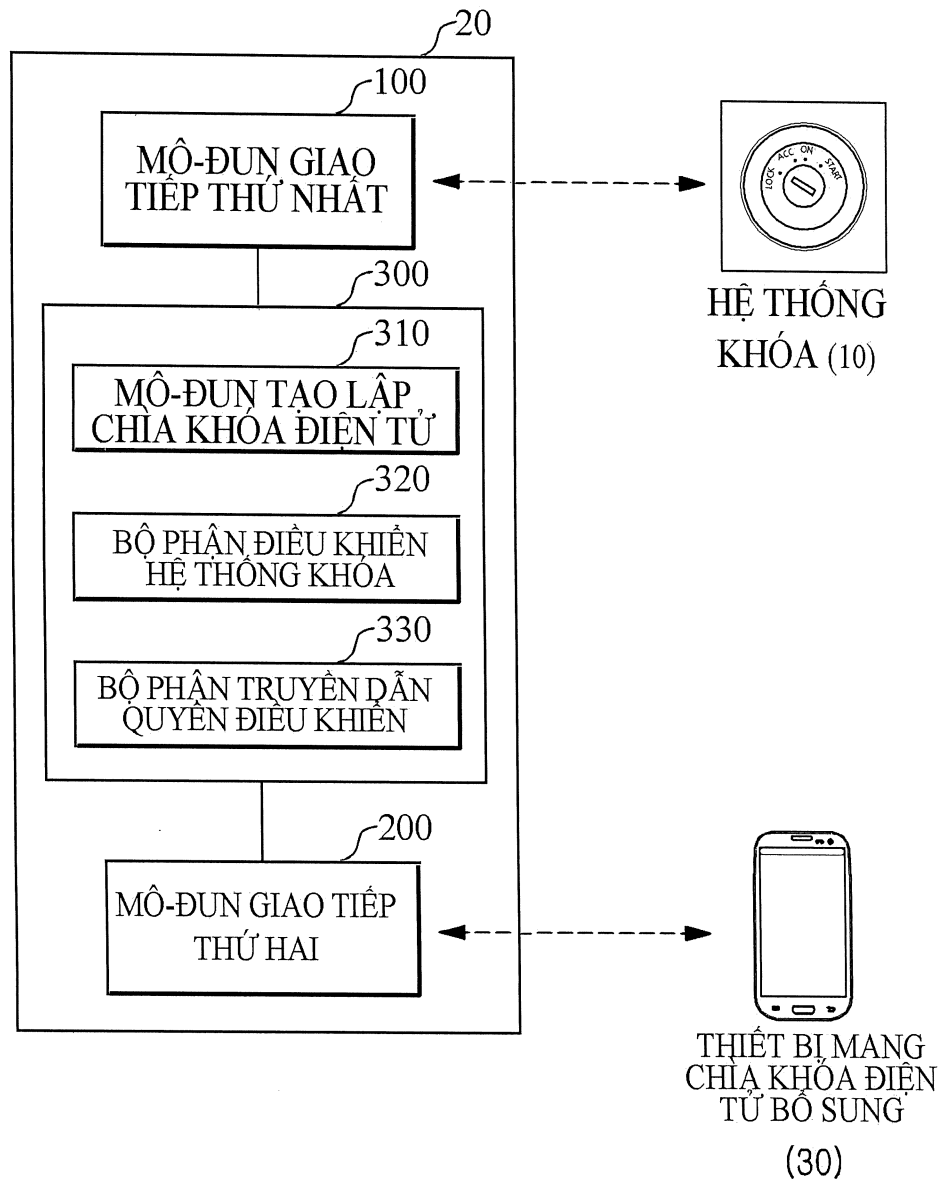


FIG.2

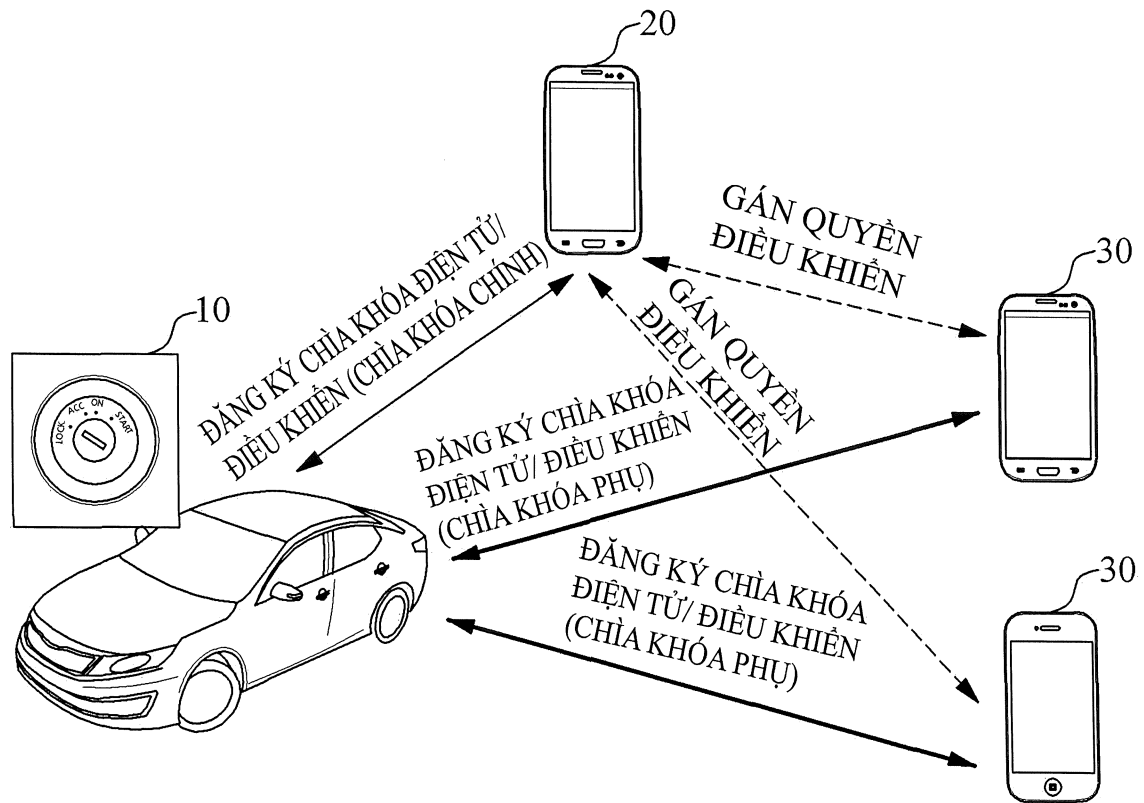


FIG.3

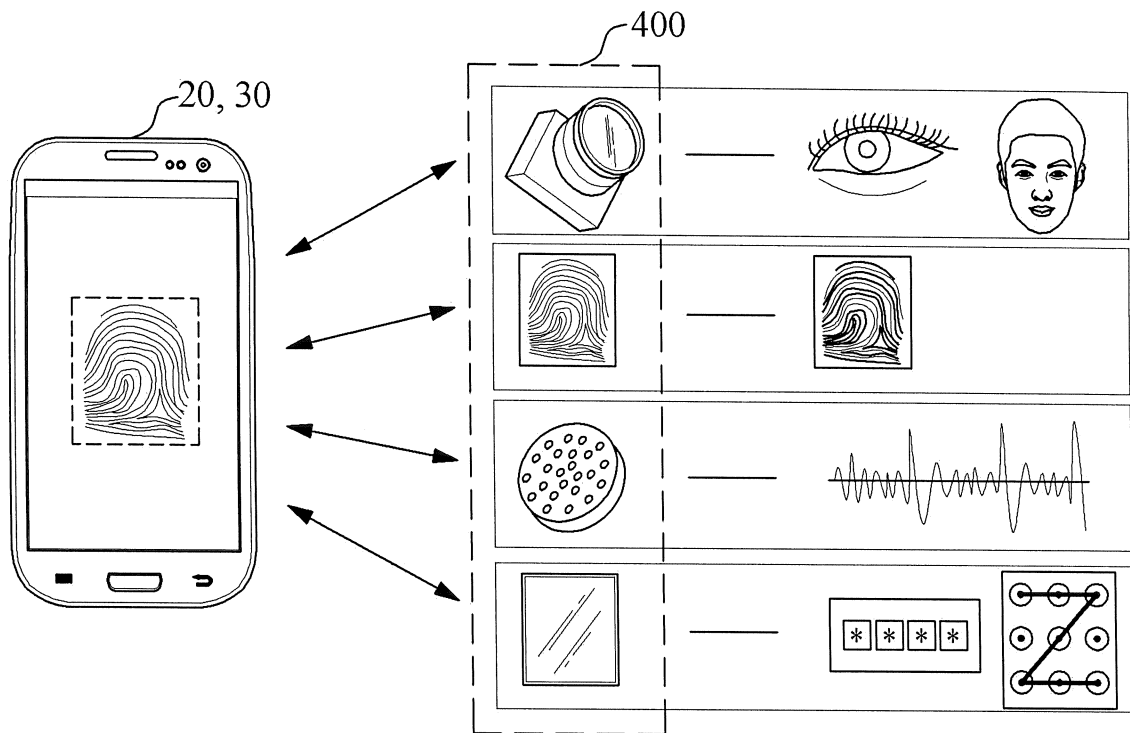


FIG.4

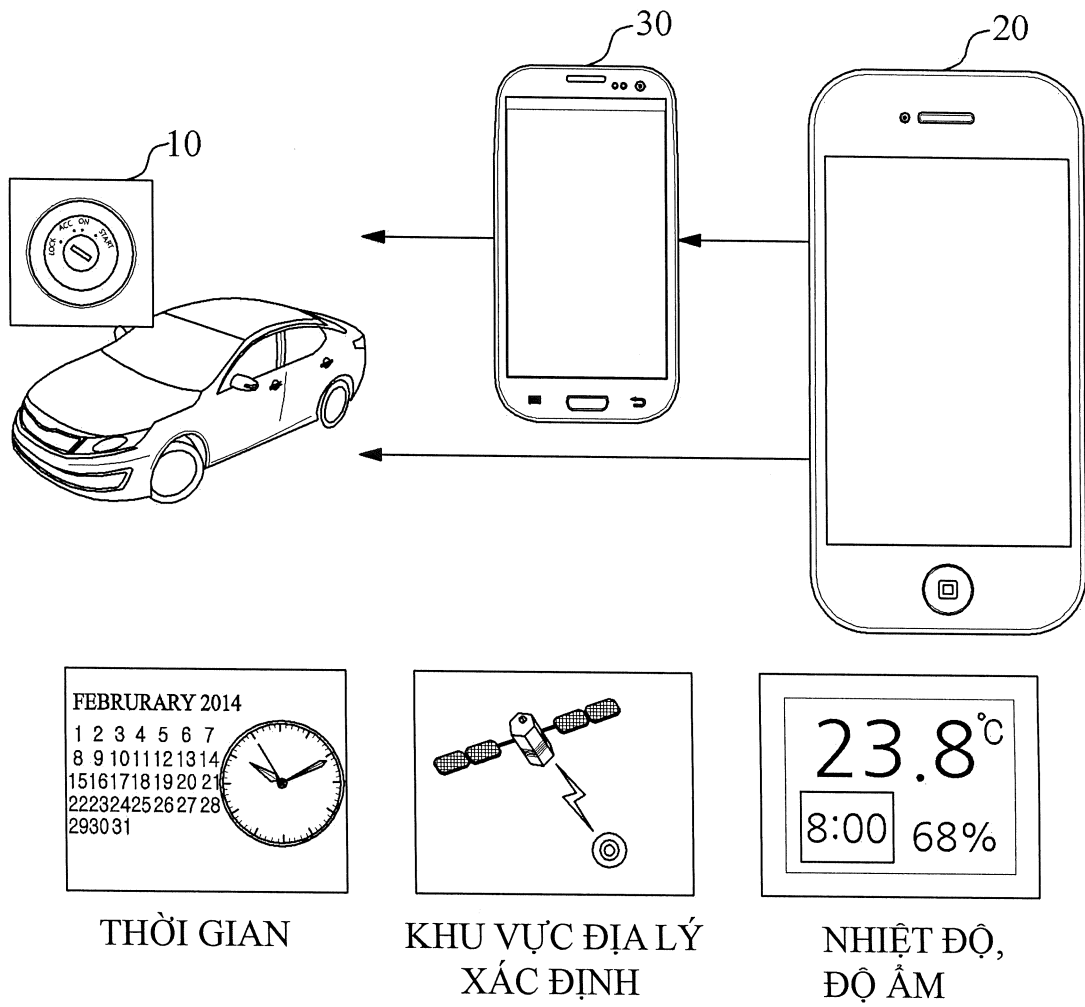


FIG.5

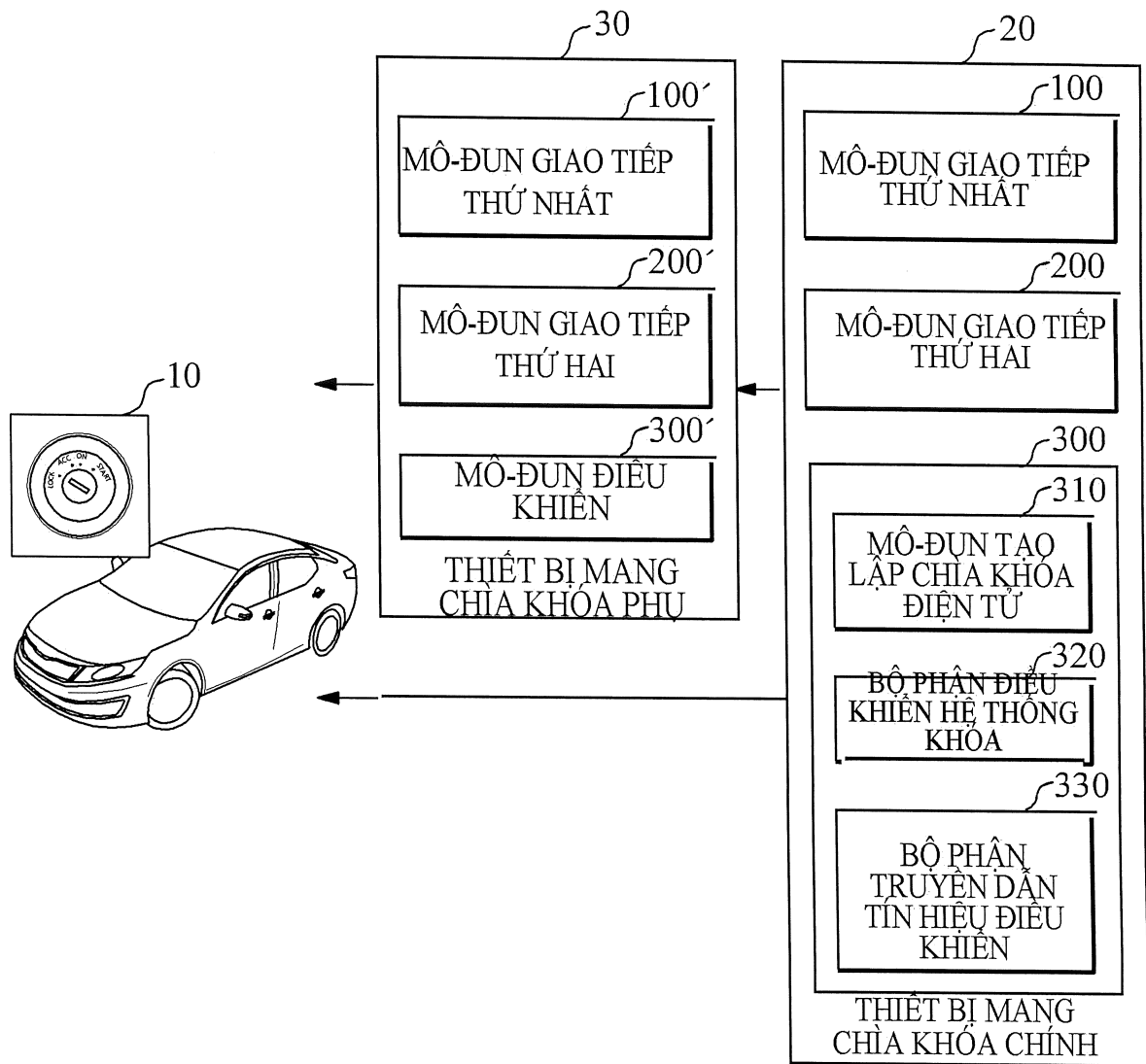


FIG.6

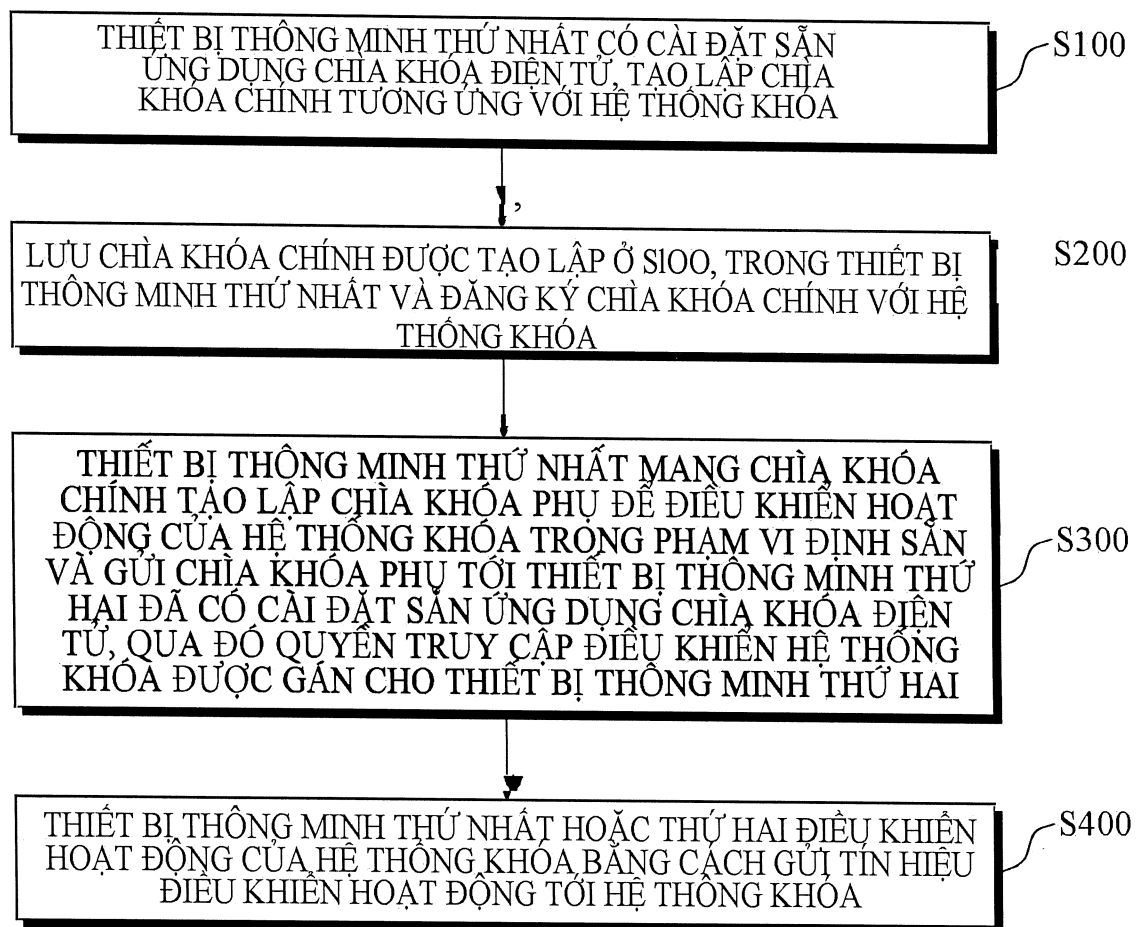


FIG.7

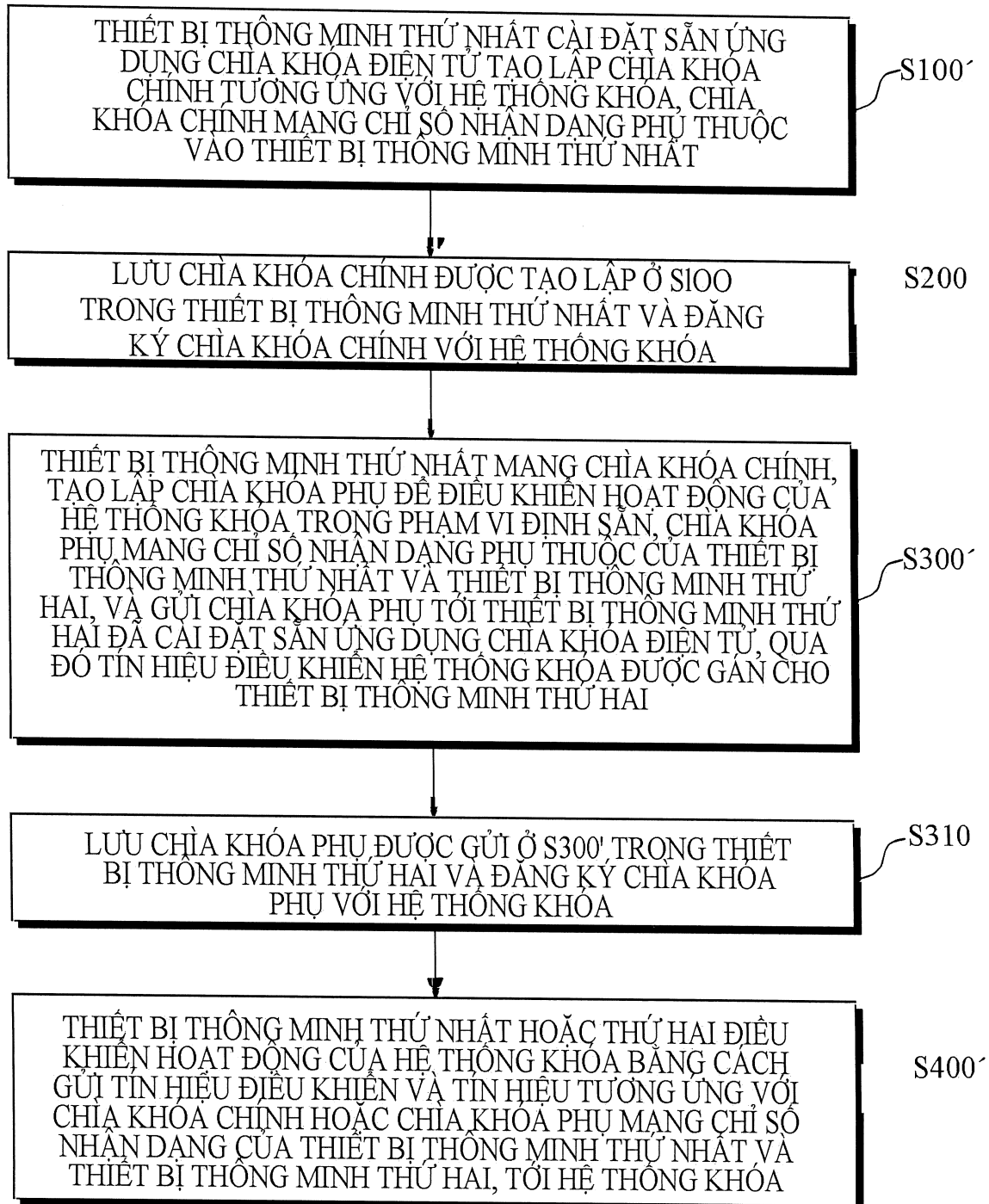
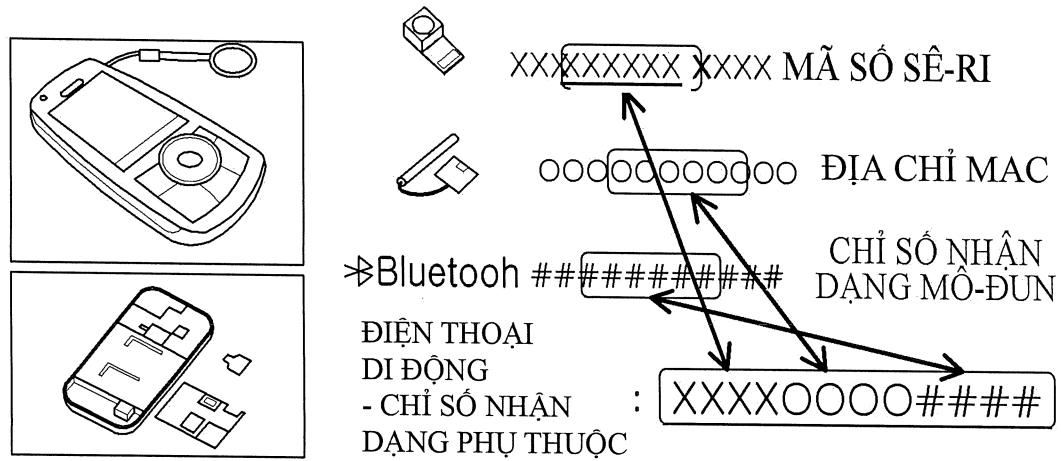


FIG.8



TAO CHỈ SỐ NHẬN DẠNG PHỤ THUỘC VÀO ĐIỆN THOẠI DI ĐỘNG BẰNG CÁCH KẾT HỢP MỘT HOẶC NHIỀU MÃ SỐ SÊ-RI CỦA MỖI MÔ-ĐUN, ĐỊA CHỈ M.A.C CỦA CARD MẠNG NỘI BỘ VÀ CHỈ SỐ NHẬN DẠNG CỦA MỖI MÔ-ĐUN